Cybersecurity in the time of Covid-19

By Indi Siriniwasa

22 Apr 2020

One of the few constants during the times we're in is the knowledge that cybercriminals will try to leverage it for their financial gain. With South Africa and a myriad of other countries locking down to limit the spread of the coronavirus, hackers are turning their attention to home networks.

Source: Josh Sorenson © from Pexels

With people either having to work from home or placed on enforced leave, the security (or lack thereof) of their computers and devices will come under intense scrutiny. Sadly, as the virus intensifies in volume and scope, so does the wave of threat attacks and campaigns that use it as bait.

Educate first

According to Trend Micro research, recent weeks have seen spam emails become the preferred method of attack, but malware and malicious URLs have also been proven to be effective.

This suggests two things – the importance of employee education when it comes to social engineering attempts, and the necessity for cybersecurity policies to directly address remote working. In the case of the latter, this must deal with where the responsibility of the company to protect an employee's device ends and where the individual's responsibility begins.

But first, the elephant in the room – employee education. This is perhaps the single-most important aspect around any defensive measures. The most technologically advanced software means nothing if a person is still lured into opening a malicious email or if they click on a compromised link.

2020 will bring even more cybersecurity challenges

Indi Siriniwasa 11 Dec 2019

Yes, cybersecurity software can help mitigate the risk of this happening by sandboxing those emails and links. However, the weakest link in the corporate security chain will always remain its people. By choosing to ignore this or minimising the effort to do so on a regular basis, the organisation leaves itself open for significant compromise especially at a time when people are working outside the relative safety of their office network.

Something as elementary as not changing the default password on a home router could potentially result in a hacker 'piggybacking' on a connection back into the corporate back-end, gaining virtually free access to sensitive data. With phishing the most common tactic employed, it is therefore imperative to do more to keep employees informed while they are working remotely. They must be trained to identify suspicious emails or links they receive and how to act appropriately. Even if this entails phoning IT staff before opening an email they are not sure about.

Keep things secure

In terms of the second point around whose responsibility it is to keep devices and networks secure, there is still some confusion around this. Many assume that their company will take care of all aspects of cybersecurity. While this is certainly true about the systems and devices accessing the network, (think employee mobile phones and tablets) the individuals themselves must accept responsibility when it comes to their home environment.

This includes everything from the home router to applying common sense such as not sharing files between unsecured systems and a work machine.

Clearly, cybersecurity at a time of the Covid-19 pandemic must be approached differently while keeping to the tenants of good practice. This is where a multi-layered defensive strategy becomes vital. Employees must not only be protected at a technological level, but also on a very human one as well.

ABOUT THE AUTHOR

Indi Siriniwasa, VP at Trend Micro Sub-Saharan Africa